



TITLE:

BDDによる計算代数・計算幾何の不変量計算 (アルゴリズムと計算の理論)

AUTHOR(S):

今井, 浩; 今井, 桂子

CITATION:

今井, 浩 ...[et al]. BDDによる計算代数・計算幾何の不変量計算 (アルゴリズムと計算の理論). 数理解析研究所講究録 1998, 1041: 12-18

ISSUE DATE:

1998-04

URL:

<http://hdl.handle.net/2433/62078>

RIGHT:

BDDによる計算代数・計算幾何の不変量計算

今井浩 (Hiroshi IMAI), 東京大学情報科学科

今井桂子 (Keiko IMAI), 中央大学情報工学科

1 はじめに

本稿では, BDD を用いてグラフや結び目の不変量を求めるアプローチ [9, 10, 14, 17, 15, 16] について, その計算代数不変量計算との関係を述べ, 集合カバー・パッキング・分割の問題の解全体の表現を BDD で効率よく表現できることを示し, 共に関連した手法として Gröbner 基底を用いたアプローチがあることを指摘する.

具体的には, まず, 2 分決定グラフ (BDD) を用いて計算代数での線形マトロイド複体の f -ベクトル, h -ベクトル (たとえば [2] 参照) が, [8] の BDD アプローチにより効率よく計算できることを指摘する. この不変量は, マトロイド複体の Stanley-Reisner 環 (たとえば [7] 参照) の Hilbert 関数と対応している ([3] など参照). Hilbert 関数計算には, これまで Gröbner 基底を用いた方法などが提案されてきている [1]. マトロイド複体の場合には, この BDD を用いた方法が有望である.

次に, 計算幾何を多次元での凸多面体の組合せ構造を扱うものまで幅広く捉えて, 集合のカバー・パッキング・分割に関する問題を軸に, 0-1 整数計画問題の実行可能解全体を BDD で効率よく表現することについて述べる. ここで基本とするのは, 単調論理関数に関するトップダウン構成アプローチ [6, 5] である. 整数計画問題の最適化部分については, BDD は全実行可能解をコンパクトに表現しており, ある目的関数に関する最適解を始点から終点への最短路として特徴づける. 整数計画問題についても, Gröbner 基底を用いた方法でその最適性テストに対する理論的解決を与えるアプローチがあり ([18] など参照), 上の場合と含め一般的な立場からその関係を見てとることができる.

以下, 分量の制限もあるので, 各々の部分について定義を中心に書いていくこととし, 結果についてはそれを示すにとどめている. 詳細については, 別の機会に譲る.

2 BDD とマトロイド複体不変量計算

2.1 マトロイド複体の f, h ベクトル

以下では, 体 F 上の $n \times m$ 行列 A の列ベクトル a_1, \dots, a_m の線形独立性に関する線形マトロイド \mathcal{M} を考える. すなわち, 独立集合族 \mathcal{I} は線形独立な列ベクトル部分集合の族である.

一般に, マトロイドの独立集合族を単体的複体とみなすことができる. 台集合 E 上, 独立集合族 $\mathcal{I} (\subseteq 2^E)$ のマトロイド $\mathcal{M} = (E, \mathcal{I})$ で, ループ (ランクが 0 の要素) がないものを考える. すると, これは

- 独立集合の部分集合は独立,
- E の各要素は \mathcal{I} に含まれる

ということで複体をなす. さらに, もちろんマトロイドの極大な独立集合は同じ要素数であるから, 純な複体になっている.

サイズが i の独立集合の数を f_i で表わす。ここで i は 0 から $m = |E|$ まで走ると考えてもよいが、実際にはマトロイドのランクが $d \equiv \rho(E)$ のとき、 $f_i = 0$ ($i > d$) となるので、以降基本的に $0 \leq i \leq d$ の f_i のみ考える。 $f_0 = 1, f_1 = |E|$ である。 (f_0, f_1, \dots, f_d) のことをマトロイドの f -ベクトルと呼ぶ。この f -ベクトルの母関数 $f(x)$ を

$$f(x) = \sum_{i=0}^d f_i x^{d-i}$$

と定める。

この $f(x)$ に対して、ここでは天下りのある $h(x)$ を次により定める。

$$h(x) = f(x-1)$$

$h(x)$ は x の多項式であり、その次数は $f(x)$ 同様に $\rho(E)$ である。 $h(x)$ の i 次項の係数を h_i で表わす：

$$h(x) = \sum_{i=0}^d h_i x^{d-i}$$

(h_0, h_1, \dots, h_d) のことをマトロイドの h -ベクトルという。詳細は [2] などに譲るが、マトロイド複体はシェリング可能であることからなどより、 $h_i \geq 0$ となる。 $h(x)$ から $f(x)$ もユニークに定まるので、独立集合族の要素数に関する情報については、 h -ベクトルは完全な情報をもっている。

2.2 マトロイド複体の Stanley-Reisner 環の Hilbert 関数

可換代数と組合せ論を結び付ける大切な構造に、単体的複体に対して定義される Stanley-Reisner 環がある。この単体的複体に対する Stanley-Reisner 環の Hilbert 級数と関係することがわかっている ([3, 7] を参照)。

まず、マトロイドの台集合 E の各要素 e_i に対して、不定元 x_i を対応させる。不定元 x_i は可換として、 E の部分集合 $\{e_{i_1}, e_{i_2}, \dots, e_{i_j}\}$ に対して項 $x_{i_1} x_{i_2} \cdots x_{i_j}$ を対応させる。

体 K の要素を係数とするこれらの不定元で構成される多項式環 $K[x_1, x_2, \dots, x_m]$ を考える ($m = |E|$)。マトロイドのサーキット族を \mathcal{C} とし、各サーキット $\{e_{i_1}, e_{i_2}, \dots, e_{i_j}\}$ に対応する項 $x_{i_1} x_{i_2} \cdots x_{i_j}$ 全体で生成されるイデアルを C とする。このイデアルによる $K[x_1, \dots, x_m]$ の剰余環 $K[x_1, \dots, x_m]/C$ を、マトロイド複体の Stanley-Reisner 環 R という。この場合の Stanley-Reisner 環の Hilbert 関数 $\text{Hilbert}(R; k)$ (k は非負整数) は、各サーキットを特性ベクトルで表わし、そのどれよりもベクトルとして以上に大きいことはない非負整数格子点で、座標の和が k となる格子点の数である。

この定義は一見わかりにくくても、例で説明することにより正確に把握できる事柄なので、次の簡単な例を考えよう。2 点を結ぶ 2 本の並列枝からなるグラフを考える。このグラフの閉路マトロイドは、サーキットは 2 本の枝で構成されるものだけで、考えている環 R は $K[x_1, x_2]/(x_1 x_2)$ である。2 次元の第一象限 (座標軸含む) の整数格子点で、サーキットに対応する $(1, 1)$ より以上に大きくない点というのは、結局 x, y 軸上の非負整数値の点のみである。したがって、 $\text{Hilbert}(R, k)$ は、 $k = 0$ のとき 1, $k \geq 1$ のとき 2 となる。図 1 参照。

Hilbert 関数は、十分大きな k に対しては k の多項式になる。

Hilbert 関数の k に関する母関数の級数を Hilbert 級数と呼び、 $\text{Hilbert}(x)$ で表す：

$$\text{Hilbert}(R) = \sum_{k=0}^{\infty} \text{Hilbert}(R, k) x^k$$

このとき、マトロイド複体の h -ベクトルと (従って f -ベクトルも) Hilbert 級数の間には、次の関係が成り立つ。

$$\text{Hilbert}(x) = \frac{1}{(1-x)^d} (h_0 + h_1 x + \cdots + h_d x^d)$$

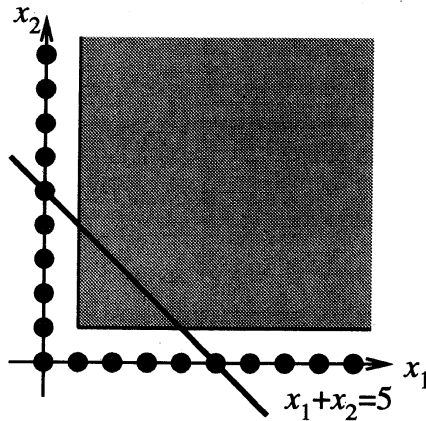


図 1: 2本の並列枝からなるグラフの開路マトロイド複体に対する Hilbert 関数の計算

以下, いくつかの例でこれらの関数の関係を見てみよう.

例 1: 2本の並列枝で結ばれる2点からなるグラフの開路マトロイド. $d = 1$ で

$$\begin{aligned} f(x) &= x + 2 \\ h(x) &= x + 1 \\ \text{Hilbert}(x) &= \frac{1}{1-x}(1+x) \\ &= 1 + 2x + 2x^2 + 2x^3 + \dots \end{aligned}$$

となる.

例 2: 3点からなる完全グラフ K_3 の開路マトロイドの場合. このとき, サークットは全体枝集合のみである. このとき,

$$\begin{aligned} f(x) &= x^2 + 3x + 3 \\ h(x) &= x^2 + x + 1 \\ \text{Hilbert}(x) &= \frac{1}{(1-x)^2}(1+x+x^2) \\ &= 1 + 3x + 6x^2 + 9x^3 + \dots \end{aligned}$$

2.3 マトロイド複体の Hilbert 級数の計算

マトロイド \mathcal{M} のランク関数を $\rho: 2^E \rightarrow \mathbf{Z}_+$ とすると, その Tutte 多項式は

$$T(\mathcal{M}; x, y) = \sum_{A \subseteq E} (x-1)^{\rho(E)-\rho(A)} (y-1)^{|A|-\rho(A)}$$

により定義される ([19] 参照). ここで, $y = 1$ を代入すると,

$$\begin{aligned} T(\mathcal{M}; x, 1) &= \sum_{A \subseteq E} (x-1)^{\rho(E)-\rho(A)} 0^{|A|-\rho(A)} \\ &= \sum_{A: |A|=\rho(A)} (x-1)^{\rho(E)-|A|} = h(x) \end{aligned}$$

となり, Tutte 多項式は $h(x)$ となる. $x = 1$ を代入すると, 双対マトロイドの h -ベクトルを与える.

Imai, Iwata, Sekine, Yoshida [8] は, 体 $\text{GF}(2)$, $\text{GF}(3)$ 上での線形マトロイドの Tutte 多項式がトップダウン構成アルゴリズムにより, その独立集合全体を表現する BDD のサイズに比例する時間で BDD が構成できることを示し, それを計算グラフとして Tutte 多項式が計算できることを示している. これを用いることにより, それらの体の上のマトロイド複体の f -ベクトル, h -ベクトル, Hilbert 関数を, 効率よく計算することができる.

3 集合カバー・パッキング・分割のBDD表現

A を $n \times m$ の 0-1 行列, b を \mathbf{Z}_+^n のベクトルとする. ここで, \mathbf{Z}_+ は非負整数の集合. このとき,

$$X^+(A, b) = \{x \mid Ax \geq b, x \in \{0, 1\}^n\}$$

$$X^0(A, b) = \{x \mid Ax = b, x \in \{0, 1\}^n\}$$

$$X^-(A, b) = \{x \mid Ax \leq b, x \in \{0, 1\}^n\}$$

と定める. $b = \mathbf{1}$ (要素が全て1のベクトル) である場合は, 台集合が行の添字集合であり, A の各列ベクトルを特性ベクトルとするような台集合の部分集合の族に対して, これらは各々集合カバー, 分割, パッキングの問題の解集合に対応する.

この $X^+(A, b)$, $X^0(A, b)$, $X^-(A, b)$ を BDD で表現すると, 対応する整数計画問題の実行可能解全てのコンパクトな表現が求まる. 以下, $b = \mathbf{1}$ の場合と, より一般の場合に分けて, この BDD を [17] のトップダウン構成することについて述べる.

3.1 b の要素が全て1の場合

この場合, $X^+(A, b)$ は m 論理変数, n 節からなる正 CNF 式のサポートとなっている. BDD での変数順を x_1, x_2, \dots, x_m とし, $\xi_l^{(k)} \in \{0, 1\}^k$ ($l = 1, 2$) を k 番目までの変数への真理値割当とする.

$A^{(k)}$ を A の第 $k+1$ 列から m 列で構成される部分行列とし, $b(\xi_l^{(k)})$ を 0 ベクトルと

$$b - \sum_{j=1}^k (\xi_j^{(k)})_j a_j$$

というベクトルの要素毎で最大値をとって得られるベクトルと定める. $b(\xi_l^{(k)}) \in \{0, 1\}^n$ である.

BDD トップダウン構成法では,

$$X^+(A^{(k)}, b(\xi_1^{(k)})) \stackrel{?}{=} X^+(A^{(k)}, b(\xi_2^{(k)}))$$

の判定ができればよい [17]. これについては, $X^+(A, b)$ は m 論理変数, n 節からなる正 CNF 式のサポートとなっていることから, [6] ([5] も参照) の結果が使える.

補題 1 ([6]): $X^+(A^{(k)}, b(\xi_1^{(k)})) = X^+(A^{(k)}, b(\xi_2^{(k)}))$ であるための必要十分条件は, それぞれで $b(\xi_l^{(k)})$ の要素が1の行の行ベクトルの集合の内, ベクトルの大小関係に関して極小なものの集合の族を考えたとき, この2つの集合族が同じになることである.

この補題とトップダウン構成法を組合せることにより, $X^+(A, b)$ を表現する BDD をその BDD サイズに比例する時間で求めることができる.

$X^-(A, b)$ は m 論理変数の負 CNF 式のサポートとして表せる. 具体的には, 行列 A を各行がクリークに対応するグラフのクリーク行列とみなし, そのグラフの安定集合としての条件を書き下せばよい. この安定集合としての論理式は負 2CNF 式となるので, 一般の CNF 式の場合よりもさらに効率のより処理が可能であり, これらのことは [6] で議論されている. $X^-(A, b)$ の BDD は, 対応するグラフで [6] の方法を使えば構成できるものの, 今の場合は A というクリーク行列が最初から与えられているので, その点を活用して, 上の補題と双対的な次の補題を得ることができる. (一般にグラフからクリーク行列を構成すると, クリーク数が指数オーダーありうることに注意.)

補題 2: $X^-(A^{(k)}, b(\xi_1^{(k)})) = X^-(A^{(k)}, b(\xi_2^{(k)}))$ であるための必要十分条件は, それぞれで $b(\xi_l^{(k)})$ の要素が0の行に現れる変数を全て0とし, 残った変数に関して, それぞれで $b(\xi_l^{(k)})$ の要素が1の行の行ベクトルの集合の内, ベクトルの大小関係に関して極大なものの集合の族を考えたとき, この2つの集合族が同じになることである.

$X^0(A, b)$ の BDD トップダウン構成では、次の補題に述べるように対応する論理関数が恒偽でないなら等価性判定は容易であるが、恒偽の判定が一般には難しく、どのような場合でもトップダウンで効率よく構成するのは難しい。

補題 3: $X^0(A^{(k)}, b(\xi_1^{(k)})) \neq \emptyset$ であるとする。このとき、 $X^0(A^{(k)}, b(\xi_1^{(k)})) = X^0(A^{(k)}, b(\xi_2^{(k)}))$ であるための必要十分条件は、 $b(\xi_1^{(k)}) = b(\xi_2^{(k)})$ である。

A が左右点部分集合のサイズが等しい 2 部グラフの接続行列である場合、これは完全マッチングの問題に対応する。完全マッチングの場合は、 $X^0(A, b)$ が空であるかどうかの判定は多項式時間で行なえるため、上の補題の簡単な等価性判定で BDD をトップダウンに出力サイズ比例で求めることができる。一方、この補題により、BDD サイズの上限を得ることはできる。

一般には、 $X^0(A, b)$ の BDD トップダウン構成は等価性判定そのものが困難になるので難しいと思われるが、実際には [6] でとられている方法を用いて、

$$X^0(A, b) = X^+(A, b) \cap X^-(A, b)$$

であることを利用して、まず $X^+(A, b)$ と $X^-(A, b)$ の BDD を各々トップダウンに求め、その 2 つの BDD を [4] などの BDD 間の AND 演算をとることによって、構成することができる。

例 3:

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad b = 1$$

に対して、

$$\xi_1^{(2)} = (1, 0)^T, \quad \xi_2^{(2)} = (0, 1)^T$$

という 2 番目の変数までの割当 2 つを考える。このとき、

$$b(\xi_1^{(2)}) = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \neq b(\xi_2^{(2)}) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

であり、それぞれの場合について、

$$\begin{aligned} X^+(A^{(2)}, b(\xi_1^{(2)})) &= X^+(A^{(2)}, b(\xi_2^{(2)})) \\ X^-(A^{(2)}, b(\xi_1^{(2)})) &\neq X^-(A^{(2)}, b(\xi_2^{(2)})) \\ X^0(A^{(2)}, b(\xi_1^{(2)})) &= X^0(A^{(2)}, b(\xi_2^{(2)})) = \emptyset \end{aligned}$$

となる。

3.2 b が一般の非負ベクトルの場合

この場合も、クリーク行列からグラフを構成するという方向で、 $X^+(A, b)$, $X^-(A, b)$ を CNF 式に書き直せば、上述の議論が適用できる。ただ、そのような変換を素朴に行なうと、一般に b の値の最大値に関してべき乗の個数の節が出てくるため、それを暗示的行なう方法が必要である。この点に関する詳細については、さらにつめる必要がある。その際には、しきい値関数をトップダウンに構成する（しかも並列化効果も高い）アルゴリズム [13] の適用についても検討する。

BDDは、全ての整数解を保持しており、線形目的関数が与えられたときの最適解を、根から1ノードへの最短路として特徴づける。これは、Gröbner基底による整数計画へのアプローチで、Graver基底など考えて与えられた整数解が最適解であるかどうか判定するテストで必要な情報を与えることと対比させることができ、興味深い。

Aの要素で2以上の整数を許す場合などへの拡張は、BEMII [12] で用いられているような算術論理式を考えることにより、行なえると思われる。実際、BEMIIでは常に算術論理式を命題論理式までおとして、そこでBDD演算 [4] を適用してこの種の問題に対する汎用アルゴリズムを与えているのであるが、そのアプローチでは中間BDDのサイズの爆発 (たとえば [11] など参照) という [4] のBDD構成アルゴリズムの本質的な困難を乗り越えることができない。このような場合に効率いいアルゴリズムを具体化して詳細に解析することは、今後の課題である。

謝辞

本研究の一部は、文部省科学研究費の援助を受けた。

参考文献

- [1] A. M. Bigatti, P. Conti, L. Robbiano and C. Traverso: A “Divide and Conquer” Algorithm for Hilbert-Poincare Series, Multiplicity and Dimension of Monomial Ideals. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lecture Notes in Computer Science, Vol.673, 1993, pp.76–88.
- [2] A. Björner: Homology and Shellability of Matroids and Geometric Lattices. In “*Matroid Applications*” (N. White, ed.), Encyclopedia of Mathematics and Its Applications, Vol.26, Cambridge University Press, 1992, pp.226–283.
- [3] J. I., Brown, C. J. Colbourn and D. G. Wagner: Cohen-Macaulay Rings in Network Reliability. *SIAM Journal on Discrete Mathematics*, Vol.9, No.3 (1996), pp.377–392.
- [4] R. E. Bryant: Graph-Based Algorithms for Boolean Function Manipulation. *IEEE Transactions on Computers*, Vol.C-35, 1986, pp.677–691.
- [5] K. Hayase and H. Imai: OBDDs of a Monotone Function and of Its Prime Implicants. *Proceedings of the 7th International Symposium on Algorithms and Computation (ISAAC’96)*, Lecture Notes in Computer Science, Vol.1178, 1996, pp.136–145; *Theory of Computing Systems*, to appear.
- [6] K. Hayase, K. Sadakane and S. Tani: Output-size Sensitiveness of OBDD Construction Through Maximal Independent Set Problem, *Proceedings of the Conference on Combinatorics and Computing (COCOON’95)*, Lecture Notes in Computer Science, Vol.959, 1995, pp.229–234.
- [7] 日比孝之: 可換代数と組合せ論. シュプリンガー・フェアラーク東京, 1995.
- [8] H. Imai, S. Iwata, K. Sekine and K. Yoshida: Combinatorial and Geometric Approaches to Counting Problems on Linear Matroids, Graphic Arrangements and Partial Orders. *Proceedings of the 2nd Annual International Computing and Combinatorics Conference (COCOON’96)*, Hong Kong, Lecture Notes in Computer Science, Vol.1090, Springer-Verlag, 1996, pp.68–80.

- [9] H. Imai, K. Sekine and K. Imai: Network Reliability Computation — Theory and Practice. *Proceedings of the IPSJ International Symposium on Information Systems and Technologies for Network Society*, World Scientific, 1997, pp.41–48.
- [10] H. Imai, K. Sekine and K. Yoshida: Binary Decision Diagrams and Generating Functions of Sets Related to Graphs and Codes. *Proceedings of the 9th IEICE Karuizawa Workshop on Circuits and Systems*, 1996, pp.91–96.
- [11] H. Imai, S. Tani and K. Sekine: Ordered Binary Decision Diagrams, Graph Theory and Computational Geometry. In “Advances in Computing Techniques: Algorithms, Databases and Parallel Processing” (H. Imai, W. F. Wong, K. F. Loe, eds.), World Scientific, Singapore, 1995, pp.69–84.
- [12] S. Minato: *Binary Decision Diagrams and Applications for VLSI CAD*. Kluwer Academic, 1996.
- [13] 丹羽純平, 定兼邦彦, 早瀬千善, 今井浩: 単調関数の OBDD のトップダウン構成の並列実装. 情報処理学会並列処理シンポジウム (*JSPP'96*), 1996, pp.161–168.
- [14] K. Sekine: *Algorithm for Computing the Tutte Polynomial and Its Applications*. Doctoral Thesis, Department of Information Science, University of Tokyo, 1997.
- [15] 関根京子, 今井浩: Tutte 多項式と Jones 多項式の計算. 京都大学数理解析研究所講究録, Vol.950, 1996, pp.133–139.
- [16] K. Sekine and H. Imai: Counting the Number of Paths in a Graph via BDDs. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, Vol.E80-A, No.4 (1997), pp.682–688.
- [17] K. Sekine, H. Imai and S. Tani: Computing the Tutte Polynomial of a Graph of Moderate Size. *Proceedings of the 6th International Symposium on Algorithms and Computation (ISAAC'95)*, Lecture Notes in Computer Science, Vol.1004, 1995, pp.224–233.
- [18] B. Sturmfels: *Gröbner Bases and Convex Polytopes*. University Lecture Series, Vol.8, American Mathematical Society, 1996.
- [19] D. J. A. Welsh: *Complexity: Knots, Colourings and Counting*, London Mathematical Society Lecture Note Series, Vol.186, Cambridge University Press, 1993.